



1835 Market Street,
Suite 1050
Philadelphia, PA 19103
(215) 279-9393
Fax: (215) 279-9394
www.flastergreenberg.com

ALEXIS ARENA, ESQUIRE

Direct Dial: (215) 279-9908

E-Mail: alexis.arena@flastergreenberg.com

October 24, 2018

VIA ECF ONLY

The Honorable Karen M. Williams
U.S. District Court, District of New Jersey
Mitchell H. Cohen Building & U.S. Courthouse
4th & Cooper Streets
Camden, NJ 08101

Re: *The HomeSource, Corp. v. Retailer Web Services, LLC, et al.*
Case No. 1:18-cv-11970-JBS-KMW

Dear Judge Williams:

Plaintiff The HomeSource Corp. (“HomeSource”) requests a telephone conference call to resolve a discovery dispute with defendant Retailer Web Services, LLC (“RWS”). RWS has refused to provide a list of its internet protocol (“IP”) addresses to help HomeSource determine if RWS was behind the cyber-attacks, hacking attacks, and other anonymous conduct launched against HomeSource in August of 2017 by the defendant John Does (“John Does”). HomeSource served an interrogatory and document request requesting this information on August 27, 2018, after consulting with its technical experts regarding what was needed to identify the Does. *See* Doc. Req. No. 16 and Interrogatory No. 18, attached hereto as Exhibit A. In response to these requests, RWS has refused to provide even a simple list of the IP addresses utilized by RWS, despite the fact that such a list is readily available.

RWS sought an extension of time to respond to HomeSource’s August 27, 2018 discovery requests, and HomeSource granted the requested extension for all requests except for HomeSource’s request for the list of RWS’s IP addresses, because that information is time-sensitive. *See* Correspondence, Ex. B at 20. Once RWS’s IP addresses are provided, HomeSource may need to subpoena identifying information from the corresponding Internet Service Providers (“ISPs”). ISPs maintain service logs that identify account holders by IP address and the date and time of the connection. This information is extremely time sensitive because ISPs only retain information concerning the identity of IP addresses for 90 to 180 days (and the attacks began on August 9, 2018), so there is a pressing need for these addresses to be produced immediately to avoid spoliation of evidence. RWS’s response to the list of IP addresses was due on October 3, 2018, before the parties’ responses to all other pending discovery requests. This is the only discovery dispute that is ripe.

HomeSource has engaged in exhaustive efforts to resolve this issue through the meet and confer process, which unfortunately has been met with severely obstructionist tactics by RWS.

The Honorable Karen M. Williams

October 24, 2018

Page 2 of 3

The parties exchanged emails related to or discussing this issue on September 6, 7, 17, 18, 19, October 3, 4, 5, 10, 15, 16, 18, 19, and 23. The parties' exhaustive, unfortunate correspondence on this issue is attached hereto as Exhibit B. The parties met in person to discuss the issue both before and after the Court conference on October 3, and Your Honor even weighed in on the issue during the Court conference on October 3. Your Honor stated that HomeSource was entitled to discovery to identify the John Does on October 3, and rejected RWS's "irrelevance" objection. HomeSource hoped at that point the dispute would be resolved and RWS's IP addresses would be forthcoming. Nevertheless, RWS has not assured HomeSource that the IP addresses will be forthcoming, has not stated when RWS's IP addresses will be forthcoming (if at all), or identified its own expert yet. If RWS delays long enough, RWS knows that the ISPs will no longer be able to identify the identity of the individuals behind the IP addresses.

The Third Circuit has not only recognized a plaintiff's right to obtain IP addresses and ISP information as relevant information in an internet John Doe case, but it has recognized that good cause exists to grant expedited discovery in these cases. *See Modern Woman, LLC v. Does I-X*, No. 2:12-CV-04858 CCCJAD, 2013 WL 888603, at *5 (D.N.J. Feb. 27, 2013) (granting expedited discovery and granting plaintiff leave to serve Rule 45 subpoenas on ISP providers to obtain the name and address of the account holder for each IP address in order to identify the John Doe defendants); *Century Media, Ltd. v. John Does I-77*, No. 2:12-CV-3911 DMCJAD, 2013 WL 868230, at *4 (D.N.J. Feb. 27, 2013) (same); *Malibu Media LLC v. Doe*, No. 1:15-CV-1129, 2015 WL 3795948, at *3 (M.D. Pa. June 18, 2015) (same). In this case, expedited discovery is not being requested because the cyber attacks and hacking began to occur after the complaint was already filed, and HomeSource was able to quickly serve discovery on RWS without a court order. However, the fact that expedited discovery is routinely granted in these cases is indicative of courts recognizing the time sensitive nature of these inquiries.

Finally, RWS continues to rely on the objection that this information is "irrelevant," because HomeSource's cyber-attack and hacking claims are currently asserted against unknown, John Doe defendants and those defendants have not yet been identified as RWS. Of course, without any discovery from RWS, it will be difficult to identify the John Does. HomeSource suspects that the John Doe defendants are RWS principals or employees, or close associates of RWS, because of the following:

1. **The Timing.** As set forth in the Amended Complaint and the parties' subsequent correspondence, these attacks by the Defendant Does, and the disparaging conduct by RWS, all occurred between mid-July 2018 (the time that RWS had a very strong financial incentive to damage HomeSource and to cause HomeSource to lose its customers) and early September 2018 (the time that the Amended Complaint was served on RWS). These cyberattacks and the hacking did not occur before or after that limited time period. In addition, the cyberattacks occurred right before key meetings between HomeSource and RWS customers. Amended Complaint, ¶ 10.
2. **The Hacking Was Based on a Consumer List only Available to RWS and HomeSource.** The **only** HomeSource customers targeted by Hacking Doe appear to be HomeSource customers that are former RWS customers. Am. Compl., ¶ 11. HomeSource

The Honorable Karen M. Williams

October 24, 2018

Page 3 of 3

possesses evidence that Hacking Doe was working from a specific, non-public list of former RWS customers. *Id.* To complete the attack, Hacking Doe manually entered information that was only available to RWS and HomeSource. *Id.* at ¶ 12. Specifically, Hacking Doe entered in the website addresses and IP addresses of customers that had switched from RWS to HomeSource, even where that information was not publicly available. *Id.*

3. **RWS Knew About the Hacking Before Anyone Else.** RWS's counsel has stated that RWS was innocently "monitoring" HomeSource's systems and identified a "security hole," which it emailed HomeSource about on July 19, 2018 at 11:58pm. *Id.* at ¶ 55. RWS has portrayed this as an attempt to "help" HomeSource. However, less than two hours later, RWS's CEO emailed the defamatory July 20th Newsletter to HomeSource's customers, stating: "Our investigation unearthed a possible major security concern with HomeSource sites." *Id.* at ¶ 56. This obviously was not a well-intentioned effort by RWS to "help" HomeSource given the timing.
4. **The Phone Call from a Fake Potential Customer.** During this time period, HomeSource's clients were also sent emails that complain about HomeSource, purportedly by anonymous "customers." *Id.* at ¶ 13-14. A "customer" ("Tony Bosco" from "Pittsburgh") also left a voicemail with HomeSource, which HomeSource traced back to a RWS phone number. *Id.* at ¶ 59-60.
5. **The Internet Traffic from within a Mile from RWS's Office.** HomeSource observed an exponentially disproportionate amount of website traffic coming from Scottsdale, Arizona. This traffic originated from the location set forth in Exhibit C to the Amended Complaint, which appears to be within a mile of RWS's office.

In sum, based on the allegations in the Amended Complaint, there is a clear basis for this discovery.

Accordingly, HomeSource respectfully requests a telephone conference with Your Honor and opposing counsel as soon as possible, so that RWS will produce its IP addresses with sufficient time for HomeSource to subpoena any ISPs as needed in order to prevent the spoliation of potential evidence.

Respectfully,

FLASTER/GREENBERG P.C.



Alexis Arena

cc: All Counsel of Record